An effective way of building cybersecurity awareness among top managers and decision makers

Kaspersky Interactive Protection Simulation

kaspersky BRING ON THE FUTURE

Learn more on kaspersky.com/awareness

Kaspersky Interactive Protection Simulation

The "People Problem"

One of the biggest security challenges is that different senior management roles view cybersecurity from dfferent perspectives, and have different priorities. This can result in a sort of decision-making "Security Bermuda Triangle":

- Business see security measures as a contradiction to their business goals (cheaper/faster/better).
- IT Security Managers may feel that cybersecurity as an infrastructure and investment issue moves outside their remit.
- Managers tasked with cost control may not see how cybersecurity spending relates to revenues and saves rather than generates cost.

Mutual understanding and partnership between these 3 are crucial to successful cybersecurity. However, traditional awareness formats, like lectures and red/blue exercises, are flawed: lengthy, overtechnical, and unsuited to busy managers, and they fail to build "common language" at the common sense level.

What is KIPS?

Kaspersky Interactive Protection Simulation (KIPS) is an exercise that places business decision makers IT security teams from corporations and government departments into a simulated business environment facing a series of unexpected cyber threats, while trying to maximize profit and maintain confidence.

The idea is to build a cyber defense strategy by making choices from amongst the best pro-active and re-active controls available. Every reaction made by the teams to the unfolding events changes the way the scenario plays out, and ultimately how much profit the company makes or fails to make.

Balancing engineering, business, and security priorities against the cost of a realistic cyberattack, the teams analyze data and make strategic decisions based on uncertain information and limited resources. If that sounds realistic, it should do, because each of the scenarios is based on real-life events.

Why KIPS is an Effective Exercise?

KIPS training is targeted at business system experts, IT people and line managers, and should increase their awareness of the risks and security problems of running modern computerized systems.

Each of the competing teams of 4–6 people is tasked with running a business consists of some production facilities and computers controlling it. During the rounds of the game, production facilities generate revenues / public welfare / business results. However, the teams also have to face cyberattacks potentially impacting enterprise performance.

In order to defend their enterprise, each team has to take strategic, managerial and technical decisions while taking operational constraints into account and maintaining a high level of revenue.

KIPS Game is a dynamic awareness program based on "learning by doing":

- Fun, engaging and fast (2 hours).
- Team-work builds cooperation.
- Competition fosters initiative & analysis skills.
- Gameplay develops understanding of cybersecurity measures.

After the KIPS Game, players come to the important and actionable conclusions for their everyday job:

- Cyberattacks hurt revenues, and need to be addressed from top-management level.
- Cooperation between IT and Business people is essential for cybersecurity success.
- Effective security budget is much smaller than revenue you risk losing, and does not require millions.
- People get used to particular security controls and its importance (audit training, anti-virus, etc).

KIPS Training Shows to Participants:

- A real role of the cybersecurity in business continuity and profitability.
- Highlights the emerging challenges and threats that are coming in nowadays.
- What are the typical mistakes companies are doing when building the cybersecurity.
- What kind of cooperation between business and security teams can help to maintain the stable operations of the enterprise and sustainability to the cyberthreats.

As the enterprise experiences a cyberattack, the players experience the impact on production and revenues, and learn to adopt different business and IT strategies and solutions in order to minimize the impact of the attack and to earn more money.

Each of the scenarios focuses on the respectful thereat vectors, allows discovering and analyzing the typical mistakes in building the cybersecurity and incident response procedures in the corresponding industry.

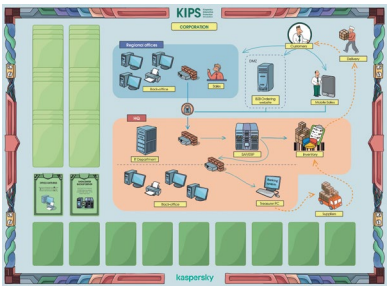
In 2019 was developed new scenario with a particular focus on protecting personal data for Local Public Administrations (LPA). Along with series of exercises and training units, KIPS LPA enables public administration employees not only to understand cybersecurity challenges, but also to transform that understanding into positive behavior models. The training also stresses how important teamwork and appropriate responsibility sharing can be and how they can help LPAs make better decisions for the security and safety of their citizens.

And the latest manufacturing scenario, which was added in the fall of 2019, is petrochemical industry.

According to the scenario each team is responsible for IT security in the new branch of a large petrochemical holding. Since the new branch has not yet managed to implement all the security procedures adopted by the holding, it becomes a weak link in the defense. The task of the teams is to ensure the normal functioning of the branch, not to lose important customers, to maintain normal relations with suppliers, to find and neutralize the sources of cyber threats.

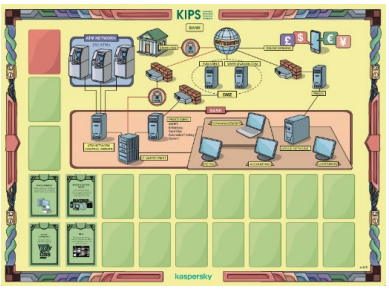
Enterprise KIPS Scenarios for All Vertical Sectors

Corporation



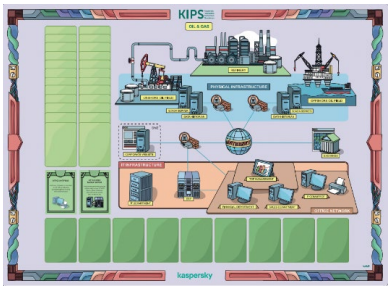
Protecting the enterprise from **ransomware, APTs, automation security flaws.**

Bank



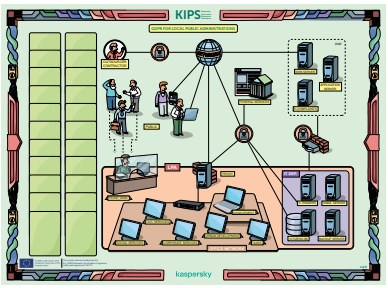
Protecting the financial institutions from **high-level emerging APTs, like Tyukpin, Carbanak.**

Oil & Gas



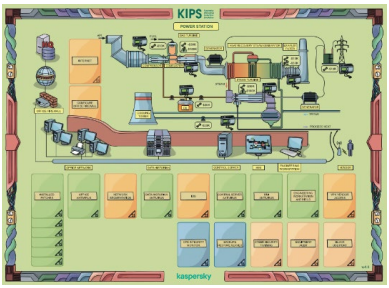
Exploring influence of variety of threats – from **website deface to a highly actual ransomware and a sophisticated APT.**

Local Public Administrations NEW!



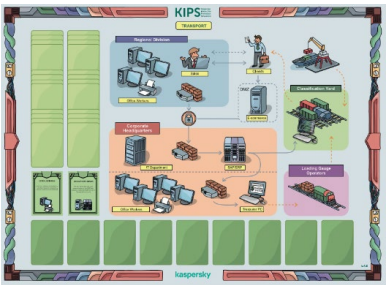
Protecting the public web servers from attacks and exploits.

Power Station or Water Plant



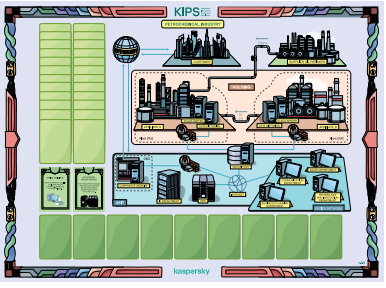
Protecting industrial control systems and critical infrastructure from **Stuxnet-style cyberattack.**

Transportation



Protecting logistic companies from **Heartbleed, APT, B2B Ransomware, Insider.**

Petrochemical industry NEW!



Ensuring the normal functioning of the new branch of a large petrochemical holding, focusing on ethylene production.

Quotes and References on KIPS Game

The Kaspersky Industrial Protection Simulation was a real eye-opener and should be made mandatory for all security professionals.

Warwick Ashford,
Computer Weekly

We at CERN have a huge number of IT and engineering systems, with thousands of people working on them. Thus, from a cybersecurity perspective, increasing awareness and engaging people to take care about cybersecurity is as crucial as the technical controls. Kaspersky training proved to be engaging, bright and efficient.

Stefan Luders,
CERN CISO

It was truly eye-opening and a number of the participants asked about using this game at their companies.

Joe Weiss PE,
CISM, CRISC, ISA Fellow

We have to build a network of people based on affiliation and cooperation and the KIPS is a perfect way how to kick it off.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, Chezh Republic

Recommendations on How to Prepare for KIPS Session

Schedule: Plan KIPS as separate event, or session inside existing event/ conference/ seminar (in this case the optimum time for KIPS is the evening of the first day).

Group: 20–100 people, split into teams of 3–4 people, ideally each team is a mix of people from Management, Engineers, CISO/IT Security:

- it is better to have at least 1 member from each role/function,
- teams may consist of people from different or the same company/ department,
- people may know each other, or may not.

Setup: The game takes 1,5 – 2 hours, but the room must be available to Kaspersky facilitator team for 2 hours prior to the game for preparation and setup.

Room: Plan ~3m2/person, no columns, regular form AV Equipment: Projector (6–8 lumens), Screen, Sound system (speakers, remote control, microphones).

Wi-Fi with internet access (for KIPS game server access), from 4Mbps iPad per each team (4 persons) with Wi-Fi support or other tablet.

Furniture: Tables of participants for 4 people (rectangular size not less than 75x180 cm, or round with no more than 1.5 m diameter), Participants should sit in groups of 4 at the tables. Tables for co-host, Chairs on the number of participants at the tables.

References and Case Studies

KIPS Game was played by industrial security professionals from 50+ countries.

- KIPS has been translated to English, Russian, German, French, Japanese, Spanish EU, Spanish LA, Portuguese, Turkish, Italian.
- KIPS was used by government agencies such as CyberSecurity
- Malaysia, Czech's NSA, Netherlands Cyber Security Centrum, to boost the awareness in the Critical Infrastructures, training hundreds of experts from national critical infrastructure companies.
- KIPS is used in enterprises like BASF (world top chemical manufacturer), CERN (Large Hadron Collider), Mitsubishi, Yokogawa, RusHydro, Panasonic, ISA (International Society of Automation), to train their own engineers, developers, customer-facing personal to note and take care about cybersecurity in the industrial automation environments.
- KIPS is licensed by leading education authorities like SANS Institute, used in the cybersecurity training programs delivered to SANS students worldwide.
- KIPS has been licensed by Security service providers and vendors, including Mitsubishi-Hitachi Power Systems, to be used as the training course for the end-customers from the Critical Infrastructure sectors.

Two Forms of KIPS Training

KIPS Live

More limitations, but stronger engagement due to on-site presence and face-to-face competition. Plays as a team-building event as well.

- Up to 80 trainees in the same room.
- The same language for all participants.
- A trainer and an assistant on site.
- Printed materials are essential.

KIPS Online

Perfect for global organizations or public activities. Can be combined with KIPS Live to add some remote teams to the on-site event.

- Up to 300 teams (= 1000 trainees) simultaneously, from any location.
- Different teams can choose a game interface in different languages.
- A trainer leads a session via WebEx.

Train-The-Trainer Available

For the cases when the customer want to use KIPS to train a wider number of employees, managers and experts from multiple departments or sites, it may be useful to purchase the license to KIPS training, educate internal trainers and run KIPS sessions at the customer own pace and convenience.

Such license is available from Kaspersky and includes:

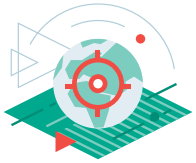
- The right to use the KIPS training program internally.
- The set of training materials and the right to use/reproduce it.
- Login/password for the KIPS software server.
- Trainer's guide, education and training for program leaders o/n how to run KIPS training.
- Maintenance and support (updates and support for KIPS software and training content).
- Optional customization of the KIPS Scenario (extra fee applies).

Kaspersky Security Awareness

Kaspersky offers computer-based training products that combine expertise in cybersecurity with best-practice educational techniques and technologies.

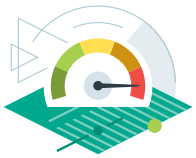
This approach changes users' behavior and helps create cybersafe environment throughout the organization.

Key program differentiators



Role-based, targeted training
- Learn what you need to know, based on your role and risk profile.
- Real-life examples and skills that can be put to immediate use.
- Learning by doing.

Human-centric
- Training that's structured in line with the way people naturally think.
- Putting a positive, proactive spin on safe behavior.
- Information and skills that are easy to digest and retain, thanks to methodologies based on the specifics of human memory.

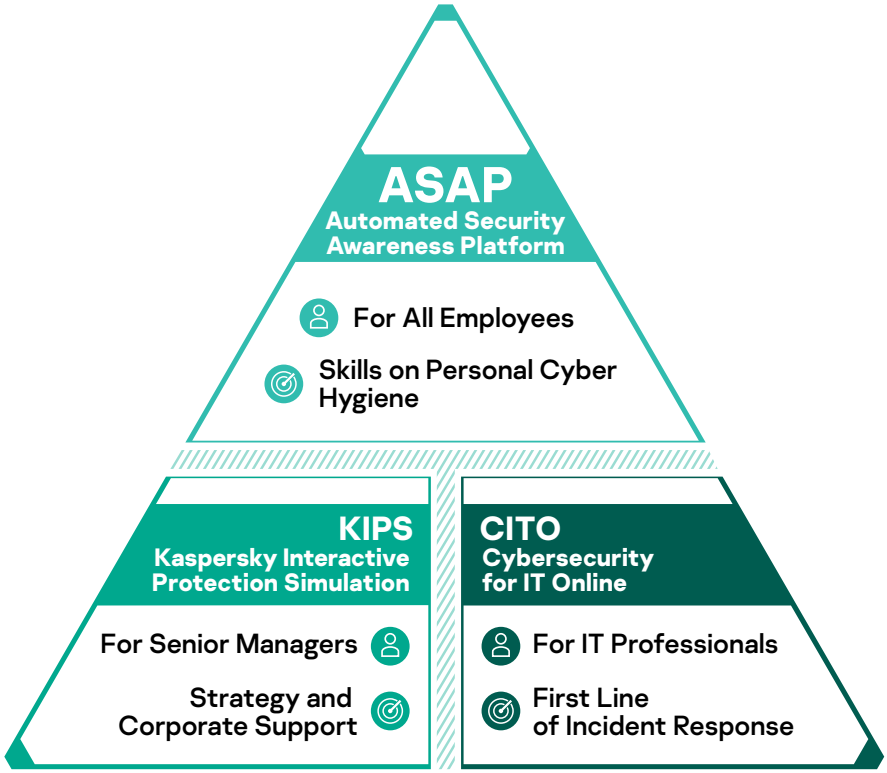


Continuous incremental learning
- From the simple to the more complex.
- Expanding and applying previously acquired knowledge in new contexts.

Easy to manage and control
- Online.
- Automated learning management.
- Invitations and motivational emails sent automatically with individual recommendations for every student.

Kaspersky Security Awareness comprises of 3 elements which intermesh, but which are also fully effective if used separately.

Different training formats for different organizational levels



Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
Product demo: www.kaspersky.com/demo-sa

www.kaspersky.com

kaspersky